This listing will replace all prior versions, and listings, of claims in the application:
LISTING OF CLAIMS:

AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for use in authenticating a service network to a station, the station having a home environment network, the method comprising:

storing a key at the service network;

transmitting information to the station from the service network that enables the station to compute the key stored at the service network;

receiving a request for service at the service network from the station;

adjusting a verification value at each ~~corresponding to key~~ usage of the key; and

transmitting information corresponding to the verification value to the station that forms a part of a verification computation enabling the station to authenticate the service network.

2. (Original) The method of claim 1, further comprising

receiving a vector of authentication information from the home environment network of the station, the vector including an indication of the vector's position in a sequence of vectors; and

wherein transmitting information to the station that enables the station to compute the key stored at the service network comprises transmitting portions of the received vector of authentication information.

3. (Original) The method of claim 2, wherein the received vector of authentication information comprises the key stored by the service network.

4. (Original) The method of claim 2, further comprising computing at the service network the key stored by the service network based on information included in the received vector.

5. (Currently amended) The method of claim 1, wherein adjusting a verification value ~~indicating use of the key~~ comprises incrementing a sequence number corresponding to a number of times the key has been used.

6. (Currently amended) The method of claim 5, wherein the verification value comprises a TSQN (Temporary Sequence Number).

7. (Original) The method of claim 1, wherein

the station comprises a cellular phone; and

the service network and home environment networks comprise cellular networks.

8. (Original) The method of claim 1, further comprising using the key to compute a cipher key for encrypting communication between the service network and the station.

9. (Original) The method of claim 1, further comprising negotiating use of a cryptographic primitive between the service network and the home environment network.

10. (Original) The method of claim 1, further comprising

transmitting a challenge to the station;

receiving a challenge response from the station; and

comparing the received challenge response with an expected response.

11. (Original) The method of claim 1, further comprising:

computing the key stored by the service network at the station;

receiving the information indicating the value corresponding to key usage at the station; and

comparing the received value with a value corresponding to key usage maintained by the station.

12. (Original) A method for use in authenticating a service network to a station, the station having a home environment network, the method comprising:

receiving information at the station from the service network;

computing a key based on the information received at the station from the service network, the computed key also being stored by the service network;

maintaining an indicator of key usage at the station;

receiving at the station an indicator of key usage maintained by the service network; and

comparing the key usage indicator maintained by the service network with the key usage indicator maintained by the station.

13. (Original) The method of claim 12, further comprising:

maintaining an authentication vector sequence number at the station;

receiving at the station from the service network an indication of an authentication vector sequence number maintained by the home environment network; and

comparing the authentication vector sequence number maintained by the home environment network with the received authentication vector sequence number maintained by the station.

14. (Original) The method of claim 13, further comprising receiving from the service network identification of a cryptographic primitive.

15. (Original) The method of claim 12, wherein

the station comprises a cellular phone; and

the service network and home environment network comprise cellular networks.

16. (Original) The method of claim 12, further comprising:

using the key to compute a cipher key for encrypting communication between the service network and the station.

17. (Original) The method of claim 12, further comprising:

receiving a challenge from the service network;

determining a challenge response; and

transmitting the challenge response to the service network.

18. (Original) The method of claim 12, wherein maintaining an indicator of key usage at the station comprises maintaining a key sequence number counter.

19. (Currently amended) A method for use in authentication in a communications network including a home environment network, a service network, and a station, the method comprising:

determining at the home environment network a cryptographic primitive offered to the home environment by the service network;
and

based on the determined cryptographic primitive, transmitting to the service network at least one vector of authentication information corresponding to a particular station.

20. (Original) The method of claim 19, wherein determining comprises receiving identification of the cryptographic primitive from the service network.

21. (Original) The method of claim 20, wherein the identification comprises a value of a MODE field.

22. (Original) The method of claim 19, wherein the vector of authentication information comprises an indication of an authentication vector sequence number maintained by the home environment network.

23. (Original) The method of claim 22, wherein the vector of authentication information comprises a challenge and an expected response.

24. (Currently amended) A method for use by a mobile station that can communicate with different service networks, the method comprising:

storing different sets of cryptographic information for the different respective service networks;

selecting ~~a set~~ one of the sets of cryptographic information for one of the service networks; and

using the one selected set of cryptographic information to communicate with the one service network.

25. (Currently amended) The method of claim 24, wherein each of the sets of cryptographic information comprises a key shared by the station and ~~the~~ a respective service network.

26. (Currently amended) The method of claim 25, further comprising computing the key shared by the station and the one service network based on information received from the one service network.

27. (Currently amended) The method of claim 25, wherein each of the sets of cryptographic information comprise an indicator of usage of the key.

28. (Original) The method of claim 27, wherein the indicator of usage comprises a sequence number.

29. (Currently amended) The method of claim 27, further comprising:

receiving from the one service network an indicator of key usage maintained by the one service network; and comparing the ~~received~~ indicator of key usage maintained by the one service network with the indicator of key usage included in the one selected set of cryptographic information.

30. (Currently amended) The method of claim 25, wherein using the one selected set of cryptographic information comprises using the one selected set of cryptographic information to authenticate the service network.

31. (Currently amended) The method of claim 25, wherein using the one selected set of cryptographic information comprises using the one selected set of cryptographic information in encrypting communication between the station and the service network.

32. (Currently amended) A method of handling authentication and key agreement in a system including a home environment network, a service network, and a mobile station, the home environment network and the mobile station sharing a secret key K, the method comprising:

determining whether the home environment and the service network share a cryptographic primitive offered by the service network;

if it is determined that the home environment and the service network do not share a cryptographic primitive, handling authentication and key agreement between the mobile station and the service network using 3GPP (Third Generation Project Partners) AKA (authentication and key agreement); and

if it is determined that the home environment and the service network share a cryptographic primitive, handling authentication and key agreement by:

computing a shared secret key (SSK);

transmitting information from the service network to the station that enables the station to compute the SSK; and

replacing the use of K in the 3GPP AKA with SSK.